



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264
27510	7590	12/07/2006	EXAMINER	
KILPATRICK STOCKTON LLP 607 14TH STREET, N.W. WASHINGTON, DC 20005			JARRETT, SCOTT L	
			ART UNIT	PAPER NUMBER
			3623	

DATE MAILED: 12/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/805,279

Applicant(s)

BARNHART, ROBERT M.

Examiner

Scott L. Jarrett

Art Unit

3623

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 October 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 29-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 29-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 10, 2006 has been entered.

Applicant's amendment amended claims 29-33. Currently claims 29-33 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 29-30 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 29 and 33 Shrader et al. teach a method and system for assisting a user in verifying a (cast) ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8):

- forming (generating, creating, signing, encrypting, etc.) a digital signature of a (cast) ballot using the private key of a system (server; "The voting tabulator signs, encrypts and sends the encrypted electronic ballot to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the validator's private key; Paragraph 0063; Figures 7-8, Element 72);

- associating (storing, linking, relating, etc.) the (cast) ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71);

Art Unit: 3623

- forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- making the message available (verification message exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- receiving the message (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8, Elements 72-74);

- extracting (decrypting, stripping, de-signing, deciphering, etc.) the ballot number and the system's digital signature from the message (verification message(s) exchanged between tabulator to mediator; Paragraph 0063; Figures 7-8, Elements 73-75);

- for vote serial number comparing the system's digital signature of the ballot received to the system's digital signature of the ballot (Paragraphs 0061-0063; Figures 7-8); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that (cast) ballot (message, token, etc.) is verified (valid, authentic, genuine, unaltered, secure, etc.; Paragraphs 0061, 0063; Figures 7-8).

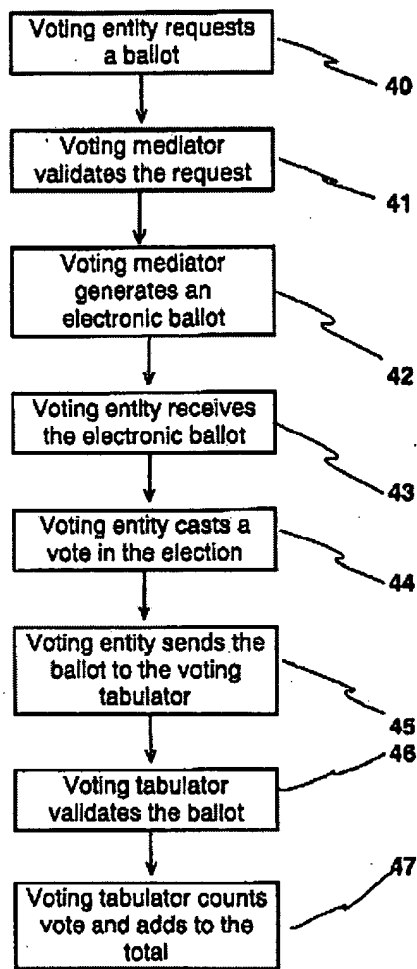


FIG. 4

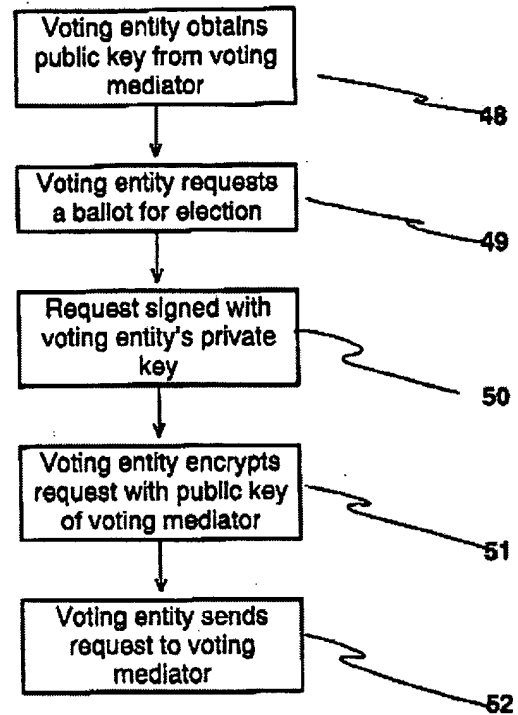
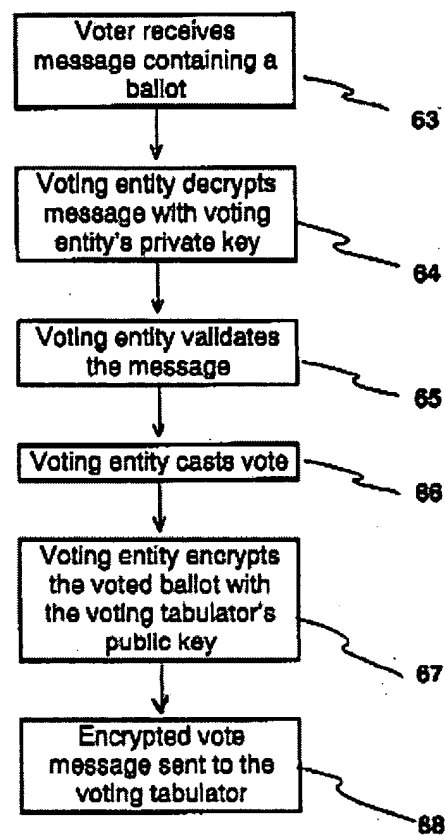
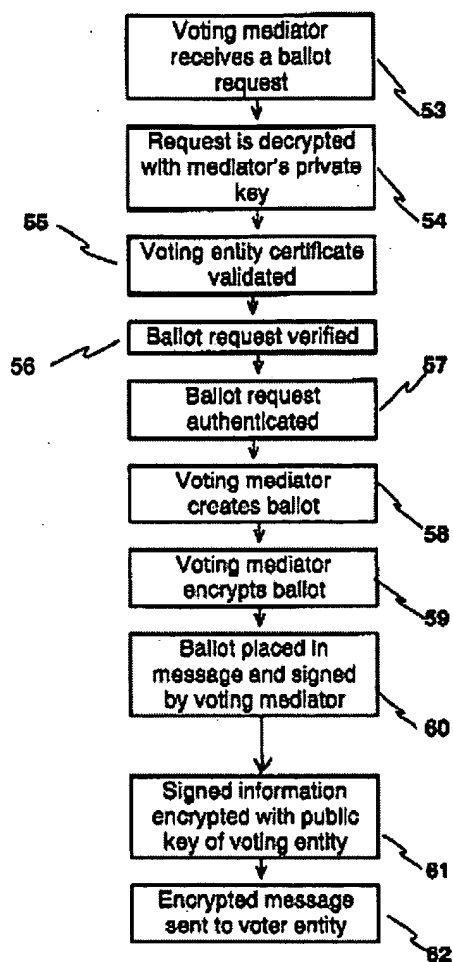
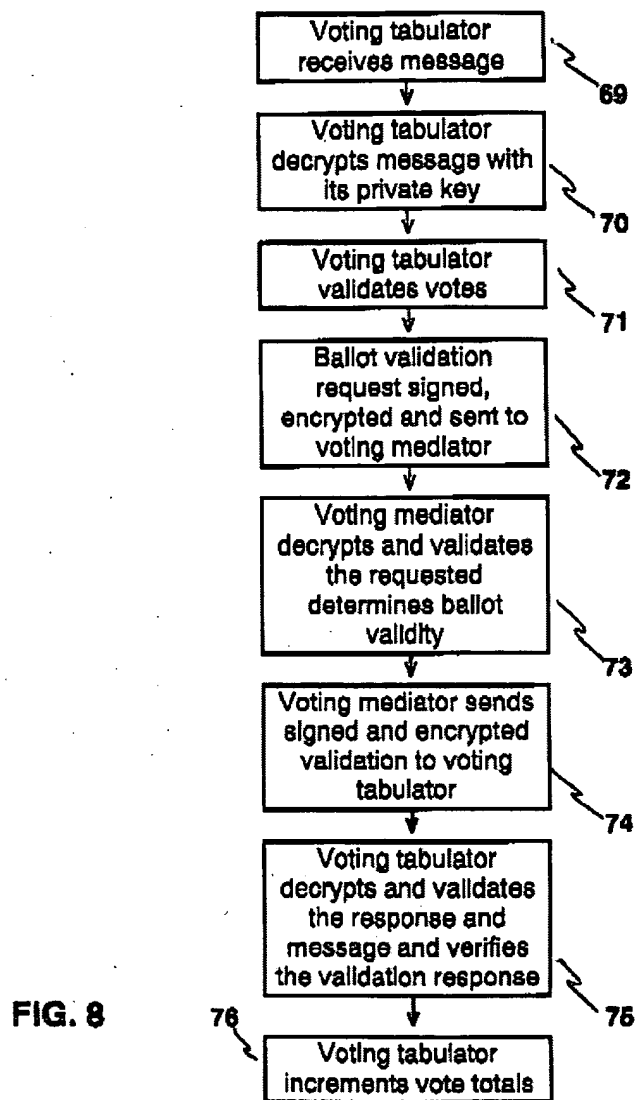


FIG. 5

Art Unit: 3623





Regarding Claim 30 Shrader et al. teach a method and system for assisting a user in verifying a ballot recorded in a system wherein the message (confirmation token, received token) further comprises the system's digital signature of the ballot and ballot number (aggregation; Paragraphs 0060-0062; Figure 2, Certificate No.); and wherein the method further comprises the steps of:

Art Unit: 3623

- extracting a digital signature of the ballot and ballot number (aggregation) from the message (received token; Paragraphs 0060, 0061, 0063; Figures 6-8); and
- the cast ballot is verified only upon the additional condition that the server's received digital signature of the aggregation is equivalent to the server's digital signature of the aggregation (Paragraphs 0061, 0063; Figures 6-8; Elements 67-75).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cranor et al., Design and Implementation of a Practical Security-Conscious Electronic Polling System (1996) in view of Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 31 Cranor et al. teach a method and system for assisting a user in verifying (validating, authenticating, certifying, etc.) a cast ballot (vote) recorded (saved, stored, etc.) in a server (system) the method/system comprising (Abstract; Figures 1,3):

- receiving, in a system (server, computer, terminal, device, etc.), at least one set of a (cast) ballot and a voter's digital signature of the ballot (Paragraph 2, Page 5);
- forming (generating, creating, signing, encrypting, etc.) a digital signature of the ballot using the private key of a system (Paragraph 2, Page 5);
- associating (storing, linking, relating, etc.) the (cast) ballot, voter's digital signature of the ballot and the voter's identification number (Paragraphs 3-4, Page 7);

Art Unit: 3623

- forming a message (confirmation token, string, receipt, acknowledgement, etc.) comprising system's digital signature of the cast ballot, the voter's digital signature of the cast ballot, and the system's digital signature of the aggregation of the cast ballot, the voter's digital signature of the ballot and the system's digital signature of the ballot ("validator", "tallier", "validation certificate", "receipt"; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- making the message (token, string, etc.) available to a user (entity, voter, system, subsystem, third party, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- receiving the messages (confirmation, token, verification, acknowledgement, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- extracting (decrypting, stripping, etc.) *at least one of the following* from the message Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

- voter's digital signature of the ballot;
 - system's digital signature of the ballot; **or**
 - system's digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation);
- for extracted ballot number and the corresponding ballot number comparing *at least one of the following* (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

Art Unit: 3623

- voter's digital signature of the ballot extracted from the message and voter's digital signature of the ballot;
- system's digital signature of the ballot extracted from the message and system's digital signature of the ballot, or
- system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation) extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation); and

- if the comparison shows equivalency (match, consistency, equality, etc.)

determining that the (cast) ballot is verified (valid, authentic, genuine, unaltered, accepted, counted, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

Cranor et al. further teaches individual verifiability (Paragraphs 1-2, Page 12) as well as a unique vote/ballot identifier (receipt number/#; Figure 1, Pages 3-4; Page 8; db index, Paragraph 1, Page 11).

Art Unit: 3623

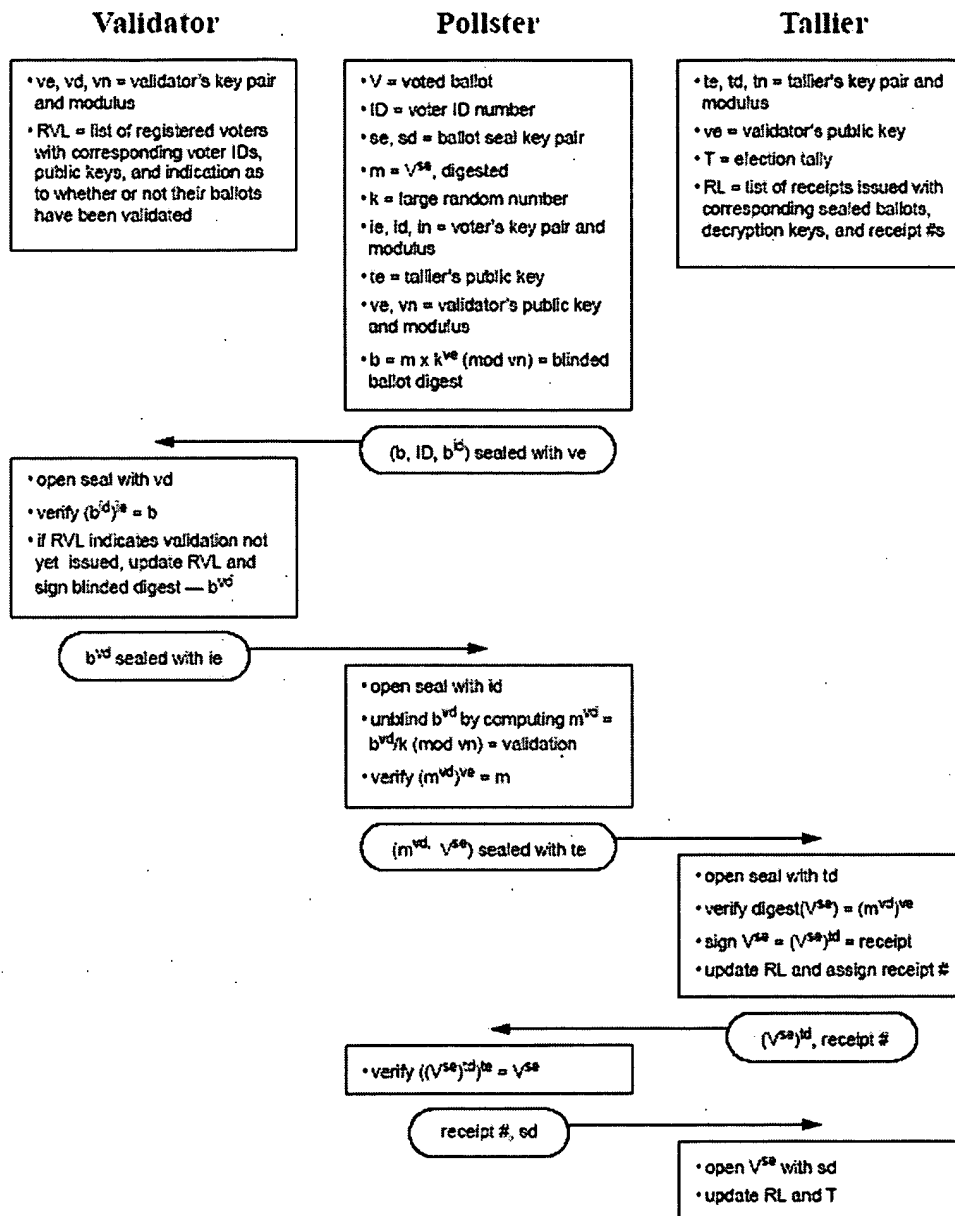


Figure 1: Blind Signature Protocol Overview

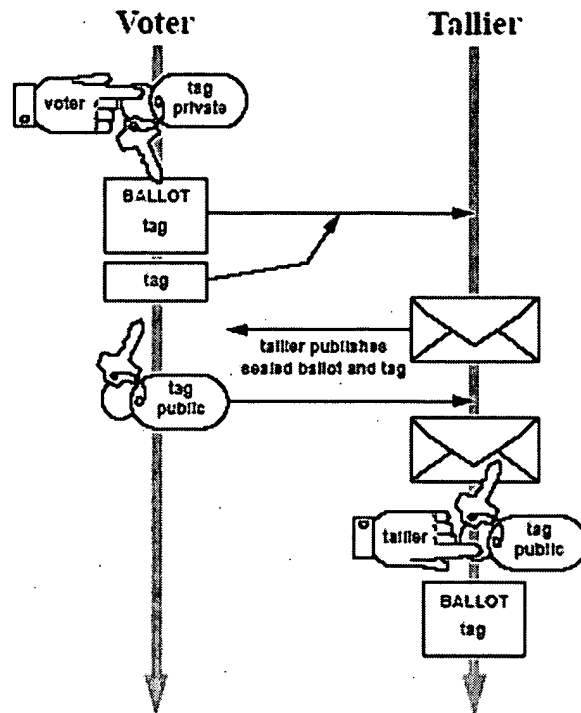


Figure 3: Phase 2 of the Two Agency Protocol

While the use of unique identifiers for (paper and/or electronic) ballots is a common practice Cranor et al. does not expressly teach that the cast ballot includes a vote serial number as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID, certificate no.) in an analogous art of secure electronic voting/balloting over a network for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 2, 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only vote once (Shrader et al.: Paragraph 0063).

Regarding Claim 32 Cranor et al. teach a method and system for verifying a cast ballot recorded in a system further comprising if the comparison shows equivalence between the system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot and the system's digital signature of the ballot (aggregation) determining that the message (token) has not been modified (altered, disturbed, edited, etc.) since its formation (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8).

Cranor et al. does not expressly teach that ballots further comprise vote serial numbers as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID) in an analogous art of secure electronic voting/balloting for the purposes of ensuring

Art Unit: 3623

voters only cast their ballot once (Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only cast their ballot once (Shrader et al.: Paragraph 0063).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Ono et al., U.S. Patent No. 6,523,115, teach a system and method for assisting a user in verifying an encrypted message/communication.

- Warther, Richard, U.S. Patent No. 6,770,727, teach a system and method for secure electronic voting comprising individual verifiability over the Internet.

- Winnett, U.S. Patent No. 6,817,515, teach a system and method for assisting users in verifying a cast ballot.

- Fujioka et al., U.S. Patent No. 6,845,447, teach a system and method for secure voting over a network comprising blind signatures, voter identification numbers, vote serial numbers (tag generator, random number given to voter).

- Reardon, U.S. Patent No. 6,968,999, teach a system and method for secure electronic voting comprising individual variability (Column 5, Lines 55-68; Figure 2, Elements 23, 24) and vote serial numbers (Column 3, Lines 23-38; Column 5, Lines 63-68; Figure 2, Elements 23, 24).

- Chung, U.S. Patent No. 7,036,730, teach a system and method for conducting secure voting including individual verifiability (Column 7, Lines 8-23; Column 8, Lines 37-55), assigning vote serial numbers before and/or after a ballot has been cast and including the vote serial numbers on the voter's receipt (Column 2, Lines 60-68; Column 3, Lines 8-30; Column 5, Lines 8-15, 56-68; Column 10, Lines 35-45; Figure 4C).

Art Unit: 3623

- Green et al., WO 01/22200 A2, teach a system and method for conducting secure voting over a network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott L. Jarrett whose telephone number is (571) 272-7033. The examiner can normally be reached on Monday-Friday, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hafiz Tariq can be reached on (571) 272-6729. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


SJ

12/5/2006


TARIQ R. HAFIZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3000